

Identity Theft & Phishing

consumer**brief**

Identity theft is the fraudulent use of your name and identifying data and occurs when your personal information is stolen and used for someone else's financial gain. Thieves will use your identity to open bank accounts and to obtain credit, merchandise or services. Victims often are left with ruined credit.

There is a new scam being used by identity thieves called "phishing." Victims are lured with e-mails disguised as official notices, and unexpected phone calls from an illegitimate company or organization asking for their personal and financial information. According to the National Consumers League, it is the fourth most common Internet scam.

WHAT INFORMATION DO THIEVES WANT?

- They want your full name, Social Security number and date of birth.
- Then, they want bank and credit card numbers and expiration dates, any financial records they can find, and even the credit card offers you receive in the mail.

HOW DO THEY STEAL MY IDENTITY?

- Thieves send you phony e-mail notices that claim to be from your bank, credit card company or a merchant and ask for your account information to solve a supposed problem.
- Unscrupulous telemarketers will convince you to give them personal information over the telephone.
- Thieves retrieve credit card receipts, bank statements, and bills from your wallets and purses and also from your garbage.
- They steal from your mailbox and even complete change of address forms to divert your mail to another location.
- Criminals will "shoulder surf"—look over your shoulder as you enter your PIN number at an ATM machine.

If you become a victim of identity theft:

- Call your police department to file a police report and keep a copy of it.
- Call the Credit Bureau Fraud Hotlines at:
Equifax **800-525-6285**
Experian **888-397-3742**
Trans Union **800-680-7289**
- Call the Federal Trade Commission Hotline to obtain its ID Theft Affidavit at: 877-438-4338



800-242-5846 • www.NJConsumerAffairs.gov

Office of the Attorney General



**New Jersey Division of
Consumer
Affairs**

WHAT DO THEY DO WITH THE INFORMATION THEY GATHER?

- Thieves use your identity to empty your bank accounts and to charge expensive items on your credit cards.
- They will open new bank accounts, credit card and store accounts and apply for loans using your name and credit history.
- They will print checks using your information and use them to go on a spending spree.
- They will establish phone and wireless services in your name.

HOW CAN I PROTECT MYSELF?

- Keep a list of all of your account numbers including your credit card numbers and expiration dates as well as the phone numbers of your creditors.
- Do NOT reply to e-mail notices, even if official-looking, that request personal or account information. Instead, call the company or go to the company's Web site if you know the correct Internet address.
- Do NOT give out your Social Security number for identity purposes, and do not carry it in your wallet.
- Do not carry extra credit cards or store charge cards in your wallet.
- Do not carry your birth certificate or passport with you unless you are traveling and it is needed for identification.
- Give NO personal information over the phone to telemarketers. If you wish to purchase something or to donate to a charity, ask them to send you a bill.
- Do not give your credit card information to companies over the phone unless you initiated the call and have a trusted relationship with the company you have called.
- When purchasing items over the Internet, give out your credit card number only after you have absolutely ensured that the Web site is a valid one and is from a company you trust. Review the company's Privacy Statement site to determine how they use information about you.
- If your wallet, credit cards or checks are stolen, cancel your accounts. When ordering new checks from your bank, pick them up rather than having them mailed to you.
- Carefully review your bank statements and bills for accuracy and contact your creditors if your usual bills do not arrive on time.

- When creating passwords and PINs, do not use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name or anything that can be easily traced to you. Do not record those numbers on anything in your wallet.
- Shred anything that has personal identification information on it including credit card or ATM receipts. Be sure to shred pre-approved credit offers that come in the mail.
- Shield your ATM or telephone key pad when using an ATM or making a phone call with your phone calling card. Some "shoulder surfers" use binoculars or video cameras to record your numbers.
- Be suspicious if you receive an e-mail that asks for your personal information.
- Never click on any link within an e-mail message requesting personal financial data - it may take you to a phony Web site. To check if the message is really from a particular company or agency, call the company directly or go to the company's Web site if you know the real Web site address.
- Never divulge your passwords, account numbers, or other sensitive information in response to any unsolicited e-mail.
- Job seekers should be particularly careful. Some "phishers" target people who list themselves on job search sites.
- If you have provided account numbers, PIN numbers, or passwords to a "phisher," notify the companies with which you have those accounts immediately.
- Be suspicious if the e-mail fails to address you by your name, has spelling or grammatical errors or warns that your account will be shut down unless you reconfirm your financial information.
- If someone calls you and says you are a victim of fraud, verify the person's identity before you provide any personal information. Ask for the person's name, the name of the company, the telephone number and the address. Then get the main number (from the phone book, the Internet or directory assistance) and call to see if the person is legitimate.

If you think you've been caught in a "phishing trap" contact the New Jersey Division of Consumer Affairs at 800-242-5846 or the Federal Trade Commission at 877- FTC-HELP.

800-242-5846 • www.NJConsumerAffairs.gov

Office of the Attorney General



**New Jersey Division of
Consumer
Affairs**